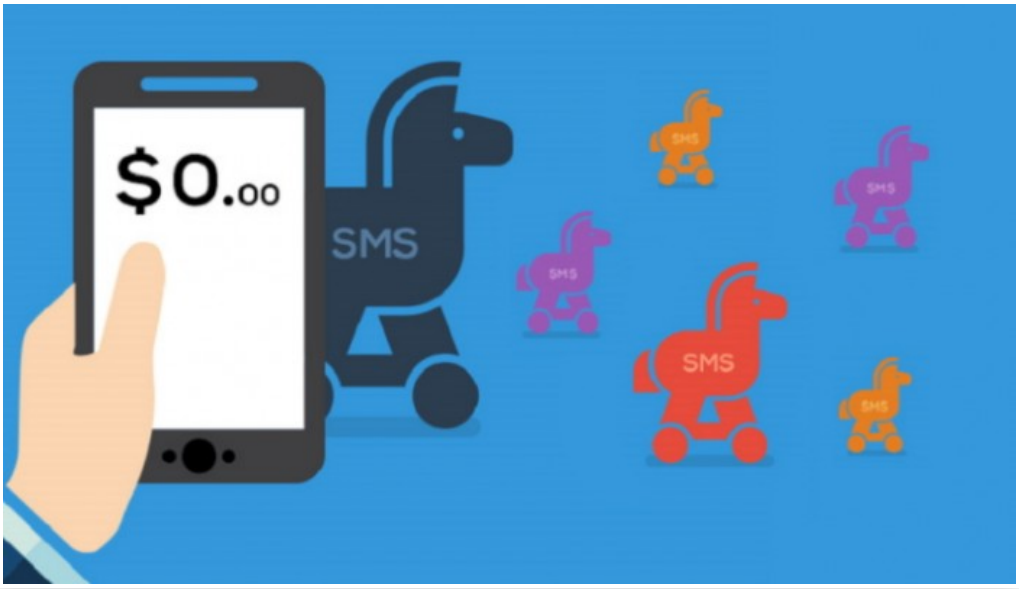
كاسبرسكي: فيروسات تروجان للمحمول تلجأ إلى أساليب قديمة لسرقة أموال المستخدمين



الأحد 1 أكتوبر 2017 11:10 م

اكتشف باحثون في كاسبرسكي لاب زيادة غير معتادة في عدد برمجيات "حصان طروادة" الخبيثة التي تسرق أموال مستخدمي الأجهزة العاملة بنظام تشغيل "أندرويد" من خلال نظام الفوترة عبر بروتوكول التطبيقات اللاسلكية WAP-billing، الذي يُعدّ نوعًا من عمليات الدفع المباشر يعمل من خلال الهواتف الذكية من دون أية عملية تسجيل.

وقالت الشركة الروسية الرائدة في مجال الأمن الإلكتروني إنه لم يُلاحظ هذا الاتجاه لفترة، لكنه أصبح منتشرًا على نحو مفاجئ في الربع الثاني من العام الجاري 2017، مؤديًا إلى تأثر الآلاف من المستخدمين في شتى دول العالم، لاسيما في الهند وروسيا.

ويُستخدم نظام الفوترة عبر بروتوكول التطبيقات اللاسلكية على نطاق واسع منذ سنوات عدة من قبل مشغلي خدمات الاتصالات المتنقلة في الاشتراكات والخدمات المدفوعة. ويحوّل هذا النوع من الدفع الرقمي كل التكاليف مباشرة إلى فاتورة هاتف المستخدم من دون الحاجة إلى تسجيل بطاقة مصرفية أو إنشاء حساب مستخدم.

وعادة ما يُحوَّيل المستخدم بعد الضغط على زر ما إلى صفحة خارجية تعرض عليه تشكيلة من الخدمات الإضافية، ليشترك بها إذا رغب عبر الضغط عليها، ومن ثَمّ يدفع تكاليف الاشتراك عبر حساب هاتفه. لكن من الممكن أن تتم كل هذه الخطوات عبر "حصان طروادة" يطبقها سرًا بالضغط بنفسه على روابط جميع الصفحات، في سيناريو تهديد حقيقي للمستخدم. بالإضافة إلى ذلك، فإن تسجيلًا بسيطًا للنطاقات في نظام فوترة مشغلي خدمات الاتصالات يسمح للمحتالين بربط صفحاتهم بنظام الفوترة بطريقة سهلة إلى حد ما وتحويل المال من حساب الضحية إلى حساباتهم.

يُذكر أن التروجان أو حصان طروادة، هو نوع من البرمجيات الخبيثة التي تظهر لكي تؤدي وظيفة مطلوبة ولكنها بدلًا من ذلك تنسخ حمولة سرية للقيام بأغراض خبيثة.

ورصدت كاسبرسكي لاب عدة عائلات من "حصان طروادة" في "أكثر 20 برنامجًا خبيثًا" انتشارًا على الهواتف تستخدم خدمة الفوترة عبر بروتوكول التطبيقات اللاسلكية. وباستطاعة كل أنواع هذه البرمجيات الخبيثة، من أجل أن تنشط نفسها عبر الإنترنت المتنقلة، تعطيل الاتصال بشبكة الإنترنت اللاسلكية (واي فاي) وتفعيل الاتصال بالإنترنت عبر بيانات مشغل الخدمة.

ويتلقى "حصان طروادة" الأكثر انتشارًا، والمنتمي لعائلة Trojan-Clicker.AndroidOS.Ubsod من البرمجيات الخبيثة، روابط من خادم التحكم والسيطرة ويفتحها. وبحسب إحصائيات "كيه إس إن"، تمكّن هذا النوع من إصابة ما يقارب 8000 مستخدم من 82 بلدًا خلال شهر يوليو الماضي.

ويستخدم برنامج خبيث آخر، في سياق سيناريو السرقة هذا، ملفات Java Script للنقر على أزرار وربطها بالفوترة عبر بروتوكول التطبيقات اللاسلكية، إذ إن بوسع "حصان طروادة" Xafekopy الذي ينتشر عبر الإعلانات التجارية متنكرًا بهيئة تطبيقات مفيدة مثل محسنات أداء البطاريات، إشراك المستخدمين بخدمات مختلفة وسرقة أموالهم. كذلك وجد خبراء كاسبرسكي لاب أن "حصان طروادة" هذا يتشابه في بعض الأوجه مع برمجية Ztorg الخبيثة، التي أعدت الشركة بشأنها تقريرًا حديثًا. وتأتي كل من برمجية Xafekopy وبرمجية Ztong الخبيثتان من منشأ يتحدث صاحبه اللغة الصينية.

بعض عائلات "حصان طروادة" الخبيثة، مثل Autisus Podecg تسيء استغلال الحقوق الخاصة بمديري النظم التقنية، ما يصعّب حذف الملفات الخبيثة، وعلاوة على ذلك، يكون بمقدور هذه البرمجيات استخدام ملفات Java Script لتجاوز اختبار "تورنج" Turing للتمييز بين

الحاسوب والإنسان، والمعروف بالاختصار CAPTCHA. فعلى سبيل المثال، ما يزال "حصان طروادة" Podec، الذي يستغل نظام الفوترة عبر بروتوكول التطبيقات اللاسلكية، نشطًا منذ العام 2015، لا سيما في روسيا، وكان ثالث أكثر البرامج الخبيثة شيوعًا في شهر حزيران/يونيو الماضي، استنادًا إلى أبحاث كاسبرسكي لاب.

وقال الخبير الأمني في كاسبرسكي لاب، رومان أونوتشيك، إن هذه الأنواع من برمجيات "حصان طروادة" الخبيثة اختفت لفترة من الوقت، لكن حقيقة عودتها وانتشارها في الآونة الراهنة قد تشير إلى أن مجرمي الإنترنت قد بدأوا في تنويع أساليب عملهم واللجوء إلى طرق فعالة، مثل نظام الفوترة عبر بروتوكول التطبيقات اللاسلكية، لاستغلال المستخدمين، فضلًا عن البرمجيات الخبيثة لعائلة SMS التي تستهدف الهواتف المحمولة ويُعتبر إنشاؤها أصعب درجة من غيرها، وأضاف: "من المثير للاهتمام استهداف البرمجيات الخبيثة لروسيا والهند بشكل رئيسي، الأمر الذي يمكن أن يُعزى إلى حالة أسواق الاتصالات المحلية. ومع ذلك، فقد اكتشفنا أيضًا مثل هذه البرمجيات في كل من جنوب إفريقيا ومصر".

وتنصح كاسبرسكي لاب المستخدمين بالانتباه إلى التطبيقات المثبتة على أجهزتهم، وتجنب تلك التي تأتي من مصادر غير معروفة، والحفاظ دائمًا على إجراء التحديثات الأمنية، من أجل منع أية أضرار محتملة والبقاء تحت الحماية في جميع الأوقات.

كذلك تقترح كاسبرسكي لاب على المستخدمين تثبيت حلول أمنية موثوق بها على أجهزتهم، مثل الحل Kaspersky Mobile Antivirus: Web Security & AppLock، الذي يهدف لحماية خصوصيتهم ومعلوماتهم الشخصية من التهديدات المحدقة بالأجهزة العاملة بنظام أندرويد.